A Practical Approach to Managing and Reducing Cyber Risks

Francesca Spidalieri
Senior Fellow for Cyber Leadership
Pell Center
Salve Regina University

@Francesca_cyber

13 March 2019
The **Internet** is increasingly connecting People, Places and Things

Disruptive Trends:
- New technological innovations (IoT, Big Data, AI, machine learning, cryptocurrency)
- Changes in the culture of the organization (mobility, virtual teams, BYOD)
- Changes in the regulations environment (new data protection & privacy regulations)
- Changes in business practices (outsourcing, decentralization, cloud computing)
- Unauthorized use of technology (unlicensed software)

*Is our organization ready for automation, disruptive technologies, and sophisticated cyber threats?*
Over the last 30 years, governments, companies, and citizens have become critically dependent on the Internet and information communications technologies BUT unfortunately, the underlying infrastructure and devices are insecure.
The Privacy Paradox: “Alexa, are we off the record?”

Everyday, the IoT is making our world more interconnected (200 billion IoT devices expected by 2025).

We will interact with an online device every 18 seconds vs. 6.5 minutes today.

We will be generating 10x more data, using, exposing, and sharing more while protecting less.

We will continue to choose convenience over privacy/security.

As technology advances, so will the prevalence and scope of cyberattacks.

Addressing cybersecurity is everyone’s business if we want to continue to live, work, and play the way we do today!
The same openness and increased reliance on the Internet that has allowed our businesses to prosper, increase efficiency and productivity, and promote economic growth has also exposed organizations to a growing number of vulnerabilities...
The big corporations may grab the headlines, but America’s SMBs have the most to lose in the aftermath of a data breach!
The Risk for Small and Midsize Companies

- The percentage of small business that experienced a **cyber attack** climbed from 61% to 67% in 2018, and 58% suffered a **data breach**, up from 54% the previous year.

- More than **61% of SMBs** suffered a successful ransomware attack, and 60% of them said the cause of the incident was a negligent employee or contractor.

- The average cost of cyber attacks on SMBs was more than **2.9 million** in 2018 (up from $2.2M the previous year), with an average cost due to **damage or theft of IT assets** of over **$1.4M**, and an average cost for **disruption to business operations** reaching more than **$1.5M**.

- An estimated **60% of SMBs** will go out of business within 6 months of a cyber attack.

**Cybercrime costs the global economy as much as $600 billion annually**

- *CSIS/McAfee Report*
The average organization takes approximately 197 days to identify that an incident has occurred and 69 days to contain it.

The number one cause of cyber breaches are a company’s own employees!
So What Can you Do to Avoid Falling Victim of a Cyber Attack?

- MINIMIZE the risks of an attack
- MONITOR for dangers
- MANAGE the damage
MINIMIZE: Enterprise-Wide Privacy + Security Program

• Create an organization-wide policy that fits the unique needs of your business
  – Privacy (e.g. access controls, use and disclosure);
  – Security (e.g. data retention, data backup, media reuse policy).

• Determine what policies, procedures, and standards need to be in place to protect your data, and applicable state and/or federal laws related to the same (compliance).

• Have a cybersecurity audit performed by an outside source and assess periodically.

• Assess collection, use and disclosure of data from:
  – Employees;
  – Clients;
  – Business Partners; and
  – Contractors, Consultants and Vendors.

• Education through training and awareness – implement awareness programs that emphasize the importance of proper “cyber hygiene” and cybersecurity as a shared responsibility.

• Examine the processing and storage of data on:
  – Mobile devices/removable media/backup media;
  – Transmission channels;
  – Applications and software;
  – Servers.

• Implement appropriate security processes to protect the transmission of data.

• Establish Website Privacy Policy and Terms of Use; Privacy Policy + Procedures; and Security Policy + Procedures.
Cyber Attacks

• It could be anyone.
• If you throw a dart at a map of the world, you are likely to hit a source of the problem.
• Experts say the risk from attacks extends beyond losing information to opening opportunities for serious damage.
• With proper systems you CAN know where every attack is originating and how frequently. Do you?

Cyber Attacks: How does this happen?

• Through your network
  – Vulnerabilities in your hardware, software or systems.
  – Your employees and mistakes they might make.
  – Your clients, if, and to the extent they have access to your network.
  – Vendors and contractors, if and to the extent they have access to your network.
MONITOR: Consider the Risks to Your Data

- **Phishing**
  - A malicious “spam-like” message sent in large batches to a broad audience.
- **Spear-Phishing**
  - A form of phishing – messages appear to come from a familiar or trusted sender and target recipients.
- **Ransomware**
  - A type of malicious software designed to block access to a computer system until a sum of money is paid.
- **Malware**
  - Software that is intended to damage or disable computers and computer systems.
MANAGE: Develop an Incident Response Plan

• Create an Incident Response and Breach Notification Plan **BEFORE** an incident occurs:
  – To be effective, the incident response plan and breach notification process must be part of a comprehensive information security program:
    • Risk assessment;
    • Trigger events;
    • Mitigation plan.
• Identify national, state, and other industry-specific laws and requirements that may apply to you (e.g., HIPAA, GDPR);
• Communications/Media Team/Vendors in Place;
• Assemble an **incident response team** and assign overall responsibility for enterprise-wide information privacy & security oversight (appoint a data privacy and a data security officer);
• Make employees aware of the important role they play in privacy and security – your employees are your **front line of defense** when it comes to security (and also one of your **biggest risks**).

“An once of prevention is worth a pound of cure” - Benjamin Franklin
MANAGE: Contain, Remove, & Recover

1. React
   - Identify the issue
   - Perform triage to determine severity

2. Respond
   - Contain the problem to minimize the impact
   - Perform forensic analysis to understand the full impact of the incident
   - Engage third-party support (if needed)
   - Notify third-parties (if needed)

3. Resolve
   - Determine and repair control deficiencies
   - Return to normal business operations
   - Conduct lessons learned

“The greatest test lies not in the crisis itself but in the ways we respond”
MANAGE: Determine legal implications under applicable data breaches notification laws

Under the **EU GDPR** a “personal data breach” is “a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data” Art. 4(12). Organizations must notify people “that a security incident has occurred” within 72 hours (if feasible) after becoming aware of the breach.

Under **U.S. state breach notification laws**, organizations must notify people if there has been a breach that exposes their unencrypted Personally Identifiable Information (PII), without undue delay.
MANAGE: Post-Incident Review

- Document all the steps and actions taken in response to the cyber incident – understand what actions worked well and those that did not;
- Conduct a follow-up session → discover, analyze, and review;
- Focus on improving processes and systems for the future, not assigning responsibility for the incident;
- Make recommendations for improvements & update incident response plan;
- Keep management informed and follow proper chain of command procedures.
MANAGE: Consider Cyber Liability Insurance

- Personally Identifiable Information
  - SSN
  - @
  - ID
  - Dog

- Financial Data
  - WWW

- Employment and Health Information
  - WWW

- 3rd Party Vendors
  - SSN
  - @
  - ID
  - WWW
How do you better protect your data beyond the enterprise-wide data privacy + security program?

MINIMIZE  MONITOR  MANAGE  BEST PRACTICE
Identify & Map Your High-Risk Data

Determine **where** your high risk data is, **where** it is going, **who** has access to it, and **how** it is being protected (and who to protect it from).

- **What Media?**
- **Where is it located?**
- **What’s the value?**
- **Is it encrypted?**
- **Where does it go?**
Set the Tone from the Top

• Integrate cybersecurity front and center into daily activities, and anchor decision-making processes in a holistic and comprehensive manner.

• Create a culture of security from the top down – Discussions about cyber risk management should be given regular and adequate time on the board meeting agenda.

• Understand how security fits into business, and business into security.

• Conduct a cybersecurity audit and a cost-benefit analysis of the potential direct and indirect costs of cyber incidents to the organizations – this may help justify increased financial and human resources dedicated to managing specific cyber risks.

• Adopt a risk-based approach.
Adopting Best-in-Practice “Cyber Hygiene” techniques means Becoming Brilliant at the Basics

• Choose strong passwords:
  – Use longer passwords or passphrases;
  – Upgrade password protection to multifactor authentication – this should be the default for every business;
  – Don’t leave your passwords unprotected (not in a post-it note or under your keyboard!)

• Install and enable a firewall;
• Regularly update antivirus and antispyware software;
• Regularly backup all important information;
• Prioritize fixing any detected weaknesses and install patches;
• Install and enable encryption on all your devices;
• Install and enable remote wiping and/or remote disabling of mobile devices;
• Disable and do not install or use file sharing applications;
• Use social media platforms wisely;
• If you use Gmail, be aware that Google mines all data and has access to all data transmitted through Gmail, according to its terms of service.
• Avoid using unsecured or public Wi-Fi – Starbucks should not replace the office!

Assume the Internet is insecure!
Create a Force Multiplier through Sharing & Networking

Member-Driven Information Sharing and Analysis Centers (ISACs)
• FS-ISAC (Financial Services)
• IT-ISAC (IT)
• MS-ISAC (State Government)
• NH-ISAC (National Health ISAC for the private sector)
• And more...

Join Forces with other Companies and Law Enforcement Agencies
• RI Joint Cybersecurity Task Force (JCTF)
• FBI/ RI InfraGard

Networking Events
• Pell Center’s RICCI events
• OSHEAN Cybersecurity Exchange Day
• Security Industry Events (RSA, Blackhat, ISC2, ISACA, etc.)
• And more...
Become familiar with applicable frameworks, benchmarks, reference guides and other independently-validated best practices to manage cyber risk

• NIST Cybersecurity Framework
• NIST Special Publication 800 series
• International Organization for Standardization (ISO) standards
• Control Objectives for Information Technology (CoBIT) standards
• EU General Data Protection Regulation (GDPR)
• SANS Institute
• ISACA
• Increase Cybersecurity Awareness and Education across the entire organization – **Cybersecurity is a shared responsibility!**
• Don’t collect data unless you need it / get rid of data as soon as of no use
• Configure your system appropriately
• Encrypt private personal data
• Back up, back up, back up

---

**Reduce Risk/Exposure (proactive measures)**

• Conduct a security audit to identify cyber risks
• Know where your “crown jewels” are and prioritize most important assets
• Monitoring and early detection
• Exercises and red teaming

---

**Risk Assessment**

• Develop a comprehensive **Enterprise Risk Management (ERM) Plan** that includes cyber risks
• Build a framework for **Incident Response** and resilience
• Develop a Business Continuity Plan (BCP)
• Data/Document Retention and Destruction Plan
• Data Security and Privacy Awareness Program

---

**Documentation/Programs**
Pell Center Website
http://pellcenter.org

‘Follow’
@PELL CENTER

‘Like’
PELL CENTER AT SALVE REGINA UNIVERSITY

Francesca Spidalieri
Senior Fellow for Cyber Leadership

Francesca.Spidalieri@salve.edu
@Francesca_cyber

www.pellcenter.org/cyber-leadership/